CLAIMS

1. A method for generating a random value, said method comprising:

monitoring a signal obtained from a communication channel, said signal including additive noise;

sampling said signal to generate a random value; and

storing said random value.

2. The method of claim 1 further comprising:

using said random value as input to a cryptographic key generation process.

3. The method of claim 1 wherein sampling comprises:

sampling at times determined by output of a linear feedback shift register.

4. The method of claim 1 wherein monitoring comprises monitoring a digital signal represented by multiple bits.

5. The method of claim 4 further comprising:

reordering said multiple bits prior to sampling.

6. The method of claim 4 wherein said digital signal comprises output of a digital to analog converter.

7. Apparatus for generating a random value, said apparatus comprising:

means for monitoring a signal obtained from a communication channel, said signal including additive noise;

means for sampling said signal to generate a random value; and

means for storing said random value.

8. The apparatus of claim 7 further comprising:

means for using said random value as input to a cryptographic key generation process.

9. The apparatus of claim 7 wherein said sampling means comprises:

means for sampling at times determined by output of a linear feedback shift register.

10. The apparatus of claim 7 wherein said means for monitoring comprises means for monitoring a digital signal represented by multiple bits.

11. The apparatus of claim 10 further comprising:

means for reordering said multiple bits prior to sampling.

12. The apparatus of claim 10 wherein said digital signal comprises output of a digital to analog converter.

13. Apparatus for generating a random value, said apparatus comprising:

a monitoring circuit that monitors a signal derived from a communication channel output; and

a register that stores a random value generated from said signal.

14. The apparatus of claim 13 further comprising:

a sampler that samples said signal to generate said random value.

15. The apparatus of claim 14 further comprising:

a linear feedback shift register that controls sampling times of said samples.

16. The apparatus of claim 14 wherein said signal comprises a digital signal.

17. The apparatus of claim 13 wherein said digital signal is represented by multiple bits and further comprising:

a bit reordering stage that reorders said multiple bits to generate said random value.

18. The apparatus of claim 16 wherein said digital signal is obtained from output of an analog to digital converter.